

## REMARKS

Claims 24, 27 and 29-46 were presented for examination. All claims stand rejected. Applicant hereby cancels all pending claims (claims 24, 27, and 29-46) without prejudice, and presents new claims 47-53. New claims 47-53 are directed to disclosed subject matter as discussed further below. Each of the Examiner's grounds of rejection will be addressed with respect to the newly-presented claims.

New claim 47 recites a computer-implemented method to facilitate management of risk related to political exposure associated with a financial transaction that includes the receipt of financial transaction data into a computer system, including data identifying a participant in the financial transaction (*see* the application as filed, *e.g.*, at page 4). A determination is made that the participant is a politically identified person by referencing data in a computer system indicating that the participant has a certain status (*see, e.g.*, page 8). Claim 47 also recites the calculation of an overall transaction political risk quotient associated with the financial transaction, which includes calculating first and second category political risk scores based on the financial transaction data (*see, e.g.*, pages 9, and 12-13). Based on a comparison of the overall transaction political risk quotient to a threshold, a suggested action is generated (*e.g.*, to decline, monitor, or gather additional information) (*see, e.g.*, page 7, stating "[i]f an account reaches or exceeds a risk quotient threshold, the system responds with a predetermined action.>").

In this manner, embodiments allow financial institutions, regulators, and other entities to manage political risk associated with financial transactions. Embodiments allow the computer-implemented identification of political risks associated with financial transactions so that remedial or preventative action can be taken. In some embodiments, these risks can be identified prior to the establishment of a financial account so that the new account can be declined if appropriate. Other remedial actions can also be taken as appropriate.

New claim 52 includes similar features. Dependent claims 48-51 and 53 recite other disclosed features (*e.g.*, as recited in the claims as originally filed).

**The Claims Comply with 35 U.S.C. §112**

The Examiner rejects claims 24, 27 and 29-46 under 35 U.S.C. §112, 1<sup>st</sup> ¶ as failing to comply with the enablement requirement.

As an initial matter, the Examiner states that "the claims recite reliance upon the 'risk quotient criteria indicative of an amount of regulatory risk' on the one hand while saying the criteria comprises an indication of whether the transaction participant comprises a politically identified person, which is a yes or no answer – not a quantified amount of risk. This language creates confusion as to what it is intended to relate." (Office Action at pages 2-3). To avoid any confusion, and to advance the case, Applicant has removed the phrase "risk quotient criteria indicative of an amount of regulatory risk".

Applicant respectfully traverses the remainder of the Examiner's rejections under 35 U.S.C. §112. In particular, the Examiner bases his rejection on his personal opinion, and ignores the clear teachings of the specification. In making his rejection, the Examiner states that there is no "detailed and tangible, concrete, full, concise, and exact written description of how one would quantify and calculate a risk quotient for regulatory risk, with regard to quantifiable aspects of a person's characteristics that could be consistently repeated by others to produce tangible and concrete results as required by this statute." (Office Action at pages 2-3). The Examiner goes on to give

"an example of the lack of enablement, where in the specifications or claims is the applicant's objective definition of all the regulatory elements involved in developing a regulatory risk quotient for someone like President Bush ... the precise objective formulas to be applied, and what is the exact objective methodology for establishing the values to be applied to each element, how would the fairness or accuracy of those objective assigned values be judged or by whom, and most importantly would the resulting risk quotient be consistent if the analysis were to be done repeatedly by two different sets of people following those detailed written steps; one set consisting of far right wing republicans and one set consisting of very liberal anti-war democrats? The answer is they could clearly not be consistent because the written enabling methodology for duplicating the invention does not exist in this application." (Office Action at pages 6-7).

Applicant respectfully asserts that his claims duly meet the proper, statutory enablement requirement. Instead, the "example" recited by the Examiner demonstrates an improper basis for a rejection and clearly runs afoul of the MPEP's unambiguous admonition against the use of personal opinion in formulating enablement rejections. Specifically, MPEP § 2164.05 explicitly and emphatically prohibits the use of personal opinion in making enablement rejections. "The examiner should never make the determination [of non-enablement] based on personal opinion. The determination should always be based on the weight of all the evidence." (MPEP § 2164.05, emphasis in original). The MPEP further instructs, "[a] specification disclosure which contains a teaching of the manner and process of making and using an invention in terms which correspond in scope to those used in describing and defining the subject matter sought to be patented must be taken as being in compliance with the enablement requirement of 35 U.S.C. 112, first paragraph, unless there is a reason to doubt the objective truth of the statements contained therein which must be relied on for enabling support." (MPEP § 2164.04, emphasis added). And finally, the MPEP provides "[a]s long as the specification discloses at least one method for making and using the claimed invention that bears a reasonable correlation to the entire scope of the claim, then the enablement requirement of 35 U.S.C. 112 is satisfied." (MPEP § 2164.01(b)).

Here, the specification discloses at least one method for making and using the claimed invention. For example, the management of risk related to political exposure associated with financial transactions is described throughout the specification as filed. Further, examples that particularly describe a method for making and using the claimed invention as recited in the newly presented claims are provided at pages 12-13. In the examples, a first category political risk score based on financial transaction data is generated for the "company profile category" (the score is -15) and a second category political risk score based on financial transaction data is generated for the account holder (the score is 3), and an overall transaction political risk quotient is calculated as the sum of  $-15 + 3 = -12$ . In the example implementation, this overall transaction political risk quotient is determined to indicate a "low risk". Appropriate action may be taken based on this determination.

This disclosed method is closely correlated to the newly presented claims. As such, the specification enables the newly presented claims. The claims are compliant with 35 U.S.C. §112. Applicant respectfully requests that the Examiner's enablement rejection be removed.

The Examiner rejected claims 37-43 and 46 under 35 U.S.C. §112, 1<sup>st</sup> ¶ for failing to comply with the written description requirement. In particular, the Examiner states that there "is no mention in the specifications of any way to consistently quantify 'veracity of previous dealings...; propensity... unlawful', or 'propensity ... unethical'."

Applicant respectfully asserts that the claims as presented complied with the written description requirement (and Applicant is further confused by the rejection since the Examiner himself specifically suggested use of this very language); however, to advance the case, Applicant has presented new claims that do not include the language noted by the Examiner. Each of the new claims is believed in compliance with all requirements of 35 U.S.C. §112 and Applicant requests that the rejections be removed.

#### **The Claimed Invention has Patentable Utility**

The Examiner rejects claims 24, 27 and 29-46 on the ground that "the claimed invention lacks patentable utility." (Office Action at page 3). In particular, the Examiner states that the "invention claims to evaluate risk associated with accounts held by a 'politically identified person'. The specifications provide very little usable clear guidance as to how to objectively make this determination." (*Id.*). The Examiner goes on to state that the "algorithms are not given nor are the necessary list of essential elements or questions identified to produce the desired tangible and concrete end result." (*Id.* at pages 3-4).

Applicant respectfully traverses this ground of rejection. In particular, Applicant respectfully asserts that the Examiner is misapplying the utility requirement of 35 U.S.C. §101, and has not established a proper prima facie case for a rejection under §101. As stated in the MPEP at §2164.07, "[t]he requirement of 35 U.S.C. 101 is that some specific, substantial, and credible use be set forth for the invention." The MPEP's guidelines for applying the utility

requirement specifically note that "[i]f at any time during the examination, it becomes readily apparent that the claimed invention has a well-established utility, do not impose a rejection based on lack of utility." (MPEP §2107 II(A)(3)). The MPEP goes on to mandate "If the applicant has asserted that the claimed invention is useful for any particular practical purpose (*i.e.*, it has 'specific and substantial utility') and the assertion would be considered credible by a person of ordinary skill in the art, do not impose a rejection based on lack of utility." (*Id.* at II(B)(1)).

Here, the newly-presented claims recite a "method to facilitate management of risk related to political exposure associated with a financial transaction" which includes, *inter alia*, the calculation of an overall transaction risk quotient that may be used to generate or determine a suggested action associated with the financial transaction. The specification, at numerous places, recites a particular practical purpose for the claimed invention – to assess political risk associated with a transaction and to recommend and/or take action in accordance with the risk. (*See, e.g.*, pages 3-4).

Despite the Examiner's personal opinion to the contrary, this particular practical purpose is not only credible in and of itself but so credible as to be in fact newsworthy. See the following quotation (among others) from Security Industry News (a respected and credible news source):

TowerGroup predicts that firms will spend about \$404 million total this year on [anti-money laundering or "AML"] solutions and services, and \$700 million through 2005. Top-tier brokerage firms seeking total package systems that cover all aspects of the Patriot Act will spend between \$25 million and \$30 million.

To start, firms typically tackle AML by risk-assessing clients according to the chances the accounts might be connected to nefarious financing. For example, out of 10 million accounts, 95 percent are rated "lower risk" while 3 percent are considered medium risk. Some firms have six categories of risk whereas others have only high and low ratings. Still others categorize by business, describing for example 12 categories of businesses and four categories of individuals. Because each of these categories has different documentation and verifications requirements, the effort can become Byzantine. (Securities Industry News, "Data Remediation looms as Huge Task" (March 24, 2003) (copy attached hereto)).

The claimed invention recites a specific, substantial, and credible use for the invention. The claimed invention is useful and statutory, and Applicant respectfully requests that the Examiner's rejection under 35 U.S.C. §101 be withdrawn.

**The Claimed Invention is Not Obvious Over the Cited Art**

The Examiner rejects all pending claims under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,341,267 ("Taub") in view of U.S. Patent No. 6,349,290 ("Horowitz") and U.S. Patent No. 6,321,212 ("Lange"). Applicant respectfully traverses this ground of rejection.

In particular, Applicant respectfully asserts that none of the references, alone or in any combination, teach or suggest a computer-implemented method to facilitate management of risk related to political exposure associated with a financial transaction which includes (a) calculating, based on first and second category political risk scores, an overall transaction political risk quotient associated with the financial transaction, or (b) comparing the overall transaction political risk quotient with a risk quotient threshold to determine a suggested action associated with the financial transaction. Each of these claimed features are missing from the cited references; further, there is simply no motivation or teaching in any of the cited references to amend or modify the references to provide these claimed features. As such, the claimed invention is patentable over the cited references, alone or in combination.

The Taub reference describes "methods, systems and apparatuses for matching individuals with behavioral requirements and for managing providers of services to evaluate or increase individual's behavioral capabilities." (See, e.g., the Title and Abstract). Taub purports to achieve a number of objects by using an "algorithm utilizing seven types of behavioral abilities to compare an individual's attained abilities with all the abilities required for any role in any situation." (Col. 5, lines 1-5). The seven types of behavioral abilities are described at Col. 8, line 59 – Col. 10, line 5, and include abilities such as spiritual abilities, ethical abilities, aesthetic abilities, physiological abilities, etc. Service providers can use the Taub system to define required behavioral abilities for a particular role situation and can then screen individuals to

select candidates who have the required behavioral abilities. That is, Taub is a personality and behavior matching system.

Taub's personality and behavior matching system is not a computer-implemented method to facilitate management of risk related to political exposure associated with a financial transaction as recited in the newly-presented claims. Applicant is at a loss to understand how the Examiner can construe Taub as describing any aspect of embodiments of the present invention. As a simple analogy: Taub's system could help Saddam Hussein (or some other politically identified person) find a job that suits his particular behavioral abilities, but it could not help a financial institution manage political risk associated with a financial transaction involving Saddam Hussein.

More particularly, Taub fails to teach or suggest calculating, based on first and second category political risk scores, an overall transaction political risk quotient associated with the financial transaction. The only scores or calculations described in Taub are scores or calculations resulting from tests taken by individuals who are having their behavioral profile monitored. There is simply no teaching or suggestion in Taub to calculate risk scores associated with political categories (e.g., such as a company profile category or an account holder category). Further, there is no teaching or suggestion to calculate an overall transaction political risk quotient based on the scores from the categories. Any suggestion that Taub does describe such features is pure hindsight reconstruction. Applicant requests that the Examiner clearly and specifically point out where there is any teaching or suggestion in Taub to perform any such scoring or calculations. Further, Taub also fails to teach or suggest any comparison of an overall transaction political risk quotient with a threshold to determine a suggested action. As discussed above, Taub does not teach or suggest generating any overall transaction political risk quotient. As such, there can be no comparison as claimed.

The Examiner combines the Horowitz reference with Taub (apparently to make up for the deficiencies of Taub). The Examiner states that Horowitz discloses the "computerized collection of personalized information (personal behavior (experience), financial aptitude, financial assets, and a combination of these factors) by a financial institution from a person with whom they are

in a financial relationship, regardless of for whom they worked or whether or not they were an elected official (politically identified person)." (Office Action at page 5). As with the rejection over Taub, the Examiner broadly points to the entire disclosure of Horowitz, without providing any specific reference to a specific teaching (citing "columns 1-48 but in particular columns 1-5"). This unclear ground of rejection makes it difficult for Applicant to directly respond to the Examiner's assertion. In reviewing the disclosure of Horowitz, it appears that Horowitz describes a system and method for "customized and personalized presentation of products and services of a financial institution." (*see, e.g.*, the Title and Abstract). In general, the Horowitz system is a targeted marketing system for "presenting customized and personalized product and service messages that allows a financial institution, such as a bank, to retain customers and attract new customers, while maintaining the lowest possible cost of agent support staff." (Col. 1, line 67 – col. 2, line 4).

Horowitz's customized and personalized sales system is not a computer-implemented method to facilitate management of risk related to political exposure associated with a financial transaction as recited in the newly-presented claims. As with the Taub reference, Applicant is at a loss to understand how the Examiner can construe the Horowitz reference as describing any aspect of embodiments of the present invention. Continuing the previous analogy: Horowitz's system could help a financial institution sell "customized and personalized" financial products to Saddam Hussein, but it could not help the financial institution manage political risk associated with a financial transaction involving Saddam Hussein.

More particularly, like Taub, Horowitz fails to teach or suggest calculating, based on first and second category political risk scores, an overall transaction political risk quotient associated with the financial transaction. Horowitz does describe the performance of some risk analyses. However, the risk analyses described by Horowitz relate to determining the customer's tolerance for risk in his financial products. Horowitz does this using a "context assessment engine 114". The context assessment engine operates to determine the "general applicability of an advice 3 to an individual, for example, by ... determining a risk level of the advice 3 based on the customer's financial profile 94, comparing the risk level to the risk tolerances to previous customers' activity, downgrading the risk tolerance of an individual in the customer profile 94, if the advice



had a risk factor involved, and updating the customer's 'life stage' factor in the customer profile 94, if the advice was aimed at a long term goal." (Col. 22, lines 6-17). Identifying or tracking a customer's tolerance for risk is not the same as calculating an overall transaction political risk quotient associated with a financial transaction.

Further, because Horowitz does not describe any calculation of an overall transaction political risk quotient, Horowitz also does not describe any comparison of an overall transaction political risk quotient with a risk quotient threshold to determine a suggested action. As with Taub, there is simply no teaching or suggestion in Horowitz to provide such features.

Finally, the Examiner cites the Lange reference, apparently to make-up for deficiencies of the Taub and Horowitz references. Again, the Examiner does not point to specific teachings of the reference, and instead broadly refers to the entire disclosure, stating that Lange "discloses (see pages 1-116 but in particular pages 1-14) a computerized method of statistically analyzing risk from financial transactions based on user data from the people involved in the financial transaction, using all the standard statistical and financial methodology. Because it would have been common sense and advantageous and would have provided a more comprehensive and cost effective method of analyzing financial risks relative to the political exposure involved it would have been obvious to one skilled in the art at the time of the invention to add the teachings of Horowitz and Lange to those of Taub, and to add those of Taub to those of the others for the same reason." (Office Action at page 5).

Lange describes a particular type of financial product (that is, a derivative instrument having a demand-based adjustable return) and a trading exchange for trading the financial product. (see, e.g., the Title and Abstract). In particular, Lange describes a derivative that can be readily traded on a public exchange. Lange's derivatives and related trading exchange are not a computer-implemented method to facilitate management of risk related to political exposure associated with a financial transaction as recited in the newly-presented claims. As with the Taub and Horowitz references, Applicant's is at a loss to understand how the Examiner can construe the Lange reference as describing any aspect of embodiments of the present invention. Lange's system could help a financial institution auction a derivative security on

behalf of Saddam Hussein, but it could not help a financial institution manage risk associated with a transaction involving Saddam Hussein.

More particularly, like Taub and Horowitz, Lange fails to teach or suggest calculating, based on first and second category political risk scores, an overall transaction political risk quotient associated with the financial transaction. There is simply no discussion of the calculation of any category risk scores, much less an overall transaction political risk score in the Lange reference. Further, Lange fails to teach or suggest comparing the overall transaction political risk quotient with a risk quotient threshold to determine a suggested action associated with the financial transaction, at least because Lange fails to teach calculating an overall transaction political risk quotient.

Each of the references lacks several elements of the claimed invention. Further, there is simply no teaching or suggestion in any of the references that would have led one skilled in the art to modify any of the references to provide the claimed features. As such, Applicant respectfully asserts that the claimed invention is patentable over the cited references, alone or in any combination. Claims 48-51 are believed patentable at least as depending from a patentable base claim. Claim 52 is believed patentable for similar reasons given for claim 47, and claim 53 is believed patentable as depending from a patentable base claim.

Applicant respectfully requests that the rejection under 35 U.S.C. §103(a) be withdrawn. If the Examiner persists in the rejection, Applicant respectfully requests that the Examiner comply with his obligation to clearly state the basis of his rejection, and clearly cite portions of the references which allegedly support his grounds of rejection so that Applicant can form an appropriate response. Applicant's previous plea for specificity (in his response to the first Office Action) has again gone unheeded.

### Miscellaneous

On September 11, 2002, Applicant submitted an Information Disclosure Statement citing a number of references from a corresponding foreign application. According to the Examiner,

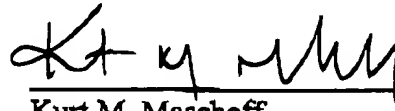
"[t]he PCT references and the IDSs are not relevant" because they "cite[s] new references, and [the] office action speaks for itself." (Office Action at page 6). Applicant respectfully requests that the Examiner consider all references that have been submitted by the Applicant. For the Examiner's convenience, the IDS (and a copy of each of the references cited therein) is resubmitted herewith.

**Conclusion**

Accordingly, Applicant respectfully asserts that each of the newly presented claims is patentable over the cited references. Applicant's silence with respect to other comments made in the Office Action does not imply agreement with those comments. If any issues remain, or if the Examiner has any further suggestions for expediting allowance of the present application, the Examiner is kindly invited to contact the undersigned via telephone at 203-972-0081.

Respectfully submitted,

December 11, 2003  
Date



Kurt M. Maschoff  
Attorney of Record  
Registration No. 38,235  
Buckley, Maschoff & Talwalkar LLC  
Five Elm Street  
New Canaan, CT 06840

Enclosure

-Securities Industry News article, dated March 24, 2003

## **Data Remediation looms as Huge Task**

Shane Kite Senior Staff Reporter

845 words

24 March 2003

Securities Industry News

English

Copyright (c) 2003 Thomson Financial, Inc. All Rights Reserved.

One of the most difficult and costly aspects of strengthened anti-money laundering (AML) regulations regards data remediation for client identification purposes, particularly for large institutions. Data remediation represents a major chunk of comprehensive compliance packages that can cost upward of \$30 million.

While the rules for enhanced due diligence on customer accounts are not retroactive (and some are still pending), firms will have to verify customer identity using specific data elements and document that process on older accounts as well as new ones to prove that they truly know their customer, according to Alan Abel, head of AML for the Americas at PricewaterhouseCoopers.

"Most folks don't realize this yet," Abel said. "To remediate all those records going back years and then to better track it electronically going forward is a huge, huge undertaking." The total number of customer accounts at large firms can reach 10 million.

One of the main caveats offered by Abel is that merely following the letter of the law will not always satisfy examiners, who may cast a suspicious eye if a firm follows the letter of the law but does not satisfy the spirit of "know your customer."

For this reason, he said, although accounts already opened are not scrutinized as much as those newly opened, firms would be wise to gather data from all accounts.

"As soon as you show or it looks like you're not reviewing your account record, you're going to have a problem," he explained. A firm's lawyers might say "Ah-ha! It said right here [in the rule] you didn't have to [gather information] until this date going forward, so we're going to draw a line in the dirt and not go beyond that." But you have to show in concept that you know your customer. If it doesn't look like you look at the file or even know what's in there, you're not making a very compelling case."

TowerGroup, the Needham, Mass.-based consultancy, agreed, and said in a report this month that identifying and integrating data residing in multiple sources is the most challenging task facing broker-dealers in complying with rules tailored from the USA Patriot Act.

"While much of the estimated effort depends on the number of unique business units a firm has, most of the actual expense comes from the effort to gather data into a centralized location, normalize it, and scrub it to ensure consistency," stated the report titled "The USA Patriot Act: Brokers Face Many Challenges in Anti-Money Laundering Compliance."

Simply closing inactive accounts can cut down on data search and storage costs once it's assured that marketing efforts aimed at reactivating the files have been exhausted, Abel suggested.

While final rules on Customer Identification Programs (CIPs) are pending, no matter the outcome the resulting regulations place brokers in the unusual position of distrusting their

customers. For this reason, many firms have chosen outside resources to crosscheck new clients against "bad guy" databases instead of initiating client interrogations. Potential customers are simply asked politely to provide more information and forms of identification and/or Tax IDs to verify identity and are ostensibly kept unaware of the background checks.

LexisNexis and the American Banker's Association announced the availability of a new database service in December called "IDPoint" for banks, joining earlier database entrants Regulatory DataCorp, formed by a consortium of Wall Street brokerages, Miami-based Worldcompliance.com and London-based World-Check.

The long-pending identity verification rules are expected next month or soon thereafter, and items considered vital to ensure identity include: name, address, date of birth and tax identification, such as a social security or employee number. While experts say it is unlikely that the final rules will require all four elements, it will be up to the firm to make a risk-based decision on whether to open the account or not without them. Congress is also still investigating the use of biometric ID cards.

TowerGroup predicts that firms will spend about \$404 million total this year on AML solutions and services, and \$700 million through 2005. Top-tier brokerage firms seeking total package systems that cover all aspects of the Patriot Act will spend between \$25 million and \$30 million.

To start, firms typically tackle AML by risk-assessing clients according to the chances the accounts might be connected to nefarious financing. For example, out of 10 million accounts, 95 percent are rated "lower risk" while 3 percent are considered medium risk. Some firms have six categories of risk whereas others have only high and low ratings. Still others categorize by business, describing for example 12 categories of businesses and four categories of individuals. Because each of these categories has different documentation and verifications requirements, the effort can become Byzantine.

"To go through and do all that if I've got 10 million accounts takes a lot," Abel said.  
Copyright 2003 Thomson Media Inc. All Rights Reserved.  
(<http://www.securitiesindustry.com>)